WHAT IS CLAIMED IS:

1. A method of managing customer security features by a security server, said method comprising:
receiving a request from a requestor;
authenticating the requestor; and
manipulating one or more security features stored in a data area corresponding to a customer in response to the request.

2. The method as described in claim 1 wherein at least one of the security features is selected from the group consisting of a photograph of the customer, a customer signature, a digital signature corresponding to the customer, a fingerprint, and a description of the customer.

3. The method as described in claim 1 further comprising:
receiving one or more new security features from the customer;
assigning an item identifier to each of the new security features; and
storing the new security features in the data area corresponding to the customer.

4. The method as described in claim 1 further comprising:
receiving an authorization from a customer, the authorization including a first merchant identifier;
storing the authorization;
receiving a retrieval request from a merchant, the retrieval request including a customer identifier

corresponding to the customer and a second merchant identifier corresponding to the merchant;

validating the merchant request, the validating including:

retrieving the authorization; and

comparing the first merchant identifier to the second merchant identifier; and

returning one or more security features corresponding to the customer in response to the first merchant identifier matching the second merchant identifier.

5. The method as described in claim 1 further comprising:

receiving an authorization from a customer, the authorization including a public key corresponding to the merchant;

storing the authorization and the merchant's public key;

receiving an encrypted retrieval request from a merchant, the encrypted retrieval request encrypted using a private key corresponding to the merchant's public key;

deciphering the encrypted retrieval request using the stored public key; and

returning one or more security features corresponding to the customer in response to the deciphering.

6. The method as described in claim 1 further comprising:

receiving an edit request from a customer, the edit request including a customer identifier and one or more updated security features, the security features each including an security item identifier;

locating a stored security feature corresponding to each of the security item identifiers; and

replacing the stored security features with the updated security features.

7. The method as described in claim 6 further comprising:

verifying the customer, the verifying including:

receiving a secret customer identifier from the customer; and

comparing the secret customer identifier with a stored secret customer identifier corresponding to the customer.

8. The method as described in claim 1 wherein the request includes an encrypted packet that is encrypted using a private key corresponding to the requestor, the method further comprising:

locating a stored public key corresponding to the requestor; and

deciphering the encrypted packet using the stored public key, the deciphering verifying the identity of the requestor, wherein the manipulating is performed in response to the encrypted packet being successfully deciphered.

9. An information handling system comprising:

one or more processors;

a memory accessible by the processors;

a network interface for communicating with other information handling systems;

one or more nonvolatile storage areas accessible by the processors; and

a security feature management tool to manage customer security features, the security feature management tool including:

means for receiving a request from a requestor;

means for authenticating the requestor;

means for manipulating one or more security features stored in a data area corresponding to a customer in response to the request.

10. The information handling system as described in claim 9 wherein the request includes an encrypted packet that is encrypted using a private key corresponding to the requestor, the information handling system further comprising:

means for locating a stored public key corresponding to the requestor; and

means for deciphering the encrypted packet using the stored public key, the deciphering verifying the identity of the requestor, wherein the manipulating is performed in response to the encrypted packet being successfully deciphered.

11. The information handling system as described in claim 9 further comprising:

means for receiving an authorization from a customer, the authorization including a first merchant identifier;

means for storing the authorization;

means for receiving a retrieval request from a merchant, the retrieval request including a customer identifier corresponding to the customer and a second merchant identifier corresponding to the merchant;

means for validating the merchant request, the validating including:

retrieving the authorization; and

comparing the first merchant identifier to the second merchant identifier; and

means for returning one or more security features corresponding to the customer in response to the first merchant identifier matching the second merchant identifier.

12. The information handling system as described in claim 9 further comprising:

means for receiving one or more new security features from the customer;

means for assigning an item identifier to each of the new security features; and

means for storing the new security features in the data area corresponding to the customer.

13. A computer program product stored on a computer operable medium for managing customer security features by a security server, said computer program product comprising:

means for receiving a request from a requestor;

means for authenticating the requestor; and

means for manipulating one or more security features stored in a data area corresponding to a customer in response to the request.

14. The computer program product as described in claim 13 wherein at least one of the security features is selected from the group consisting of a photograph of the customer, a customer signature, a digital signature corresponding to the customer, a fingerprint, and a description of the customer.

15. The computer program product as described in claim 13 further comprising:
means for receiving one or more new security features from the customer;
means for assigning an item identifier to each of the new security features; and
means for storing the new security features in the data area corresponding to the customer.

16. The computer program product as described in claim 13 further comprising:
means for receiving an authorization from a customer, the authorization including a first merchant identifier;
means for storing the authorization;
means for receiving a retrieval request from a merchant, the retrieval request including a customer identifier corresponding to the customer and a second merchant identifier corresponding to the merchant;
means for validating the merchant request, the validating including:
retrieving the authorization; and
comparing the first merchant identifier to the second merchant identifier; and

means for returning one or more security features corresponding to the customer in response to the first merchant identifier matching the second merchant identifier.

17. The computer program product as described in claim 13 further comprising:

means for receiving an authorization from a customer, the authorization including a public key corresponding to the merchant;

means for storing the authorization and the merchant's public key;

means for receiving an encrypted retrieval request from a merchant, the encrypted retrieval request encrypted using a private key corresponding to the merchant's public key;

means for deciphering the encrypted retrieval request using the stored public key; and

means for returning one or more security features corresponding to the customer in response to the deciphering.

18. The computer program product as described in claim 13 further comprising:

means for receiving an edit request from a customer, the edit request including a customer identifier and one or more updated security features, the security features each including an security item identifier;

means for locating a stored security feature corresponding to each of the security item identifiers; and means for replacing the stored security features with the updated security features.

19. The computer program product as described in claim 18 further comprising:

means for verifying the customer, the verifying including:

means for receiving a secret customer identifier from the customer; and

means for comparing the secret customer identifier with a stored secret customer identifier corresponding to the customer.

20. The computer program product as described in claim 13 wherein the request includes an encrypted packet that is encrypted using a private key corresponding to the requestor, the computer program product further comprising:

means for locating a stored public key corresponding to the requestor; and

means for deciphering the encrypted packet using the stored public key, the deciphering verifying the identity of the requestor, wherein the manipulating is performed in response to the encrypted packet being successfully deciphered.